Software Automation for Reverse Engineering Complex Microcircuits

Michael Strizich
MicroNet Solutions Inc. – Pix2Net Software
10501 Research Rd. Albuquerque NM 87123
mstriz@micronetsol.net Ph. 505-765-2498

Abstract

The reverse engineering of VLSI microcircuits is becoming more of a requirement for both government and commercial practices when it comes to electronic part obsolescence, patent infringement and trusted operation. In order to reconstruct these complex systems, and a multi-disciplined team that ranges from circuit designers, metallurgical experts and a software suite that integrates and automates many of these disciplines.

Introduction

Reverse engineering (RE) state-of-the art microchips is very difficult at best given the small dimensions, density of transistors and number of metal layers (Billions of nodes of information to track). It's analogous to DNA mapping, and if you now add anti-tamper, memory code extraction and obfuscation, it becomes much more complex.

The primary reasons behind reverse engineering a microchip are Patent Infringement Assessments, Electronic Part Obsolescence (remake), Security Evaluations, and Trusted Design evaluations to name a few.

The continuous drive of Moore's law to increase the integration level of silicon chips has presented major challenges to the reverse engineer demanding new and more sophisticated software and technology to analyze chips.

This presentation gives an overview of reverse engineering software which automates SEM transistor identification, library cell extraction, net listing, and schematic generation integrated into one software suite.

The software suite automates the RE process by using new neural networking image recognition software algorithms capable of converting and stacking metal & via layers while converting them to GDS II on the fly. The software is very flexible, and designed to either import image tiles, or capture the tiles by controlling Nano-Stages and SEM parameters.

The functional description, schematics, library catalog, and GDS stack-up can be exported to common CAD software packages.

Automated Reverse Engineering Steps

Reverse Engineering (RE) of microchips consists of transforming physical layers into a functional electrical model. This requires delayering the many sandwiched layers that make-up interconnects and active components within the microchip. The sequential flow is as follows:

1) Delayering (Expose) Interconnects (metal / via's)
2) Diffusion / Implants (transistors)
3) Stitch Tiles (Mosaic) / Overlay and Align Layers
4) Convert to GDS II
5) Extract Library Cell Catalog
6) Netlist – Schematic Generation
7) Hierarchal Models
8) Microcode Memory Extraction

Delayering Interconnects:

Delayering is one of the most difficult steps. The challenge is to remove very small amounts of material, typically a 0.5 micron or less while keeping the region of interest planar. The larger the die area, the more difficult this step can be. The goal is to expose the metal line and via at each interconnect level which will shorten the length of time required for SEM tile extraction.

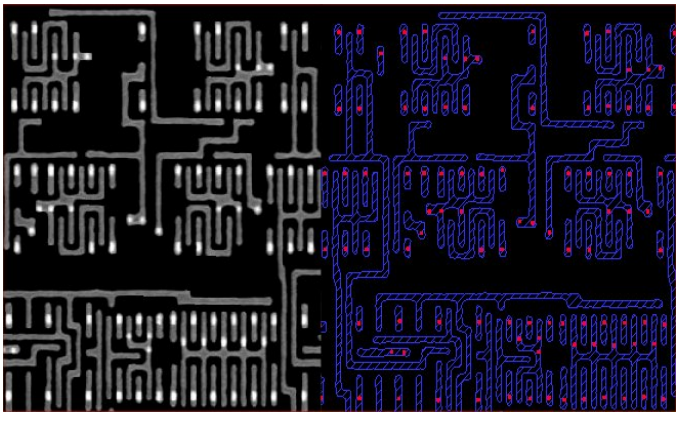


Figure 1: Metal / Via SEM Tile converted to GDS II.

Diffusion / Implant "Hi-Lighting":

To automate the library catalog extraction, the active layers (n or p) that make up the transistors need to be identified. This can be done using chemical staining, Electron Beam Induced Current (EBIC), or intrinsic voltage contrast. This information will be used by the software when the transistors are automatically identified.

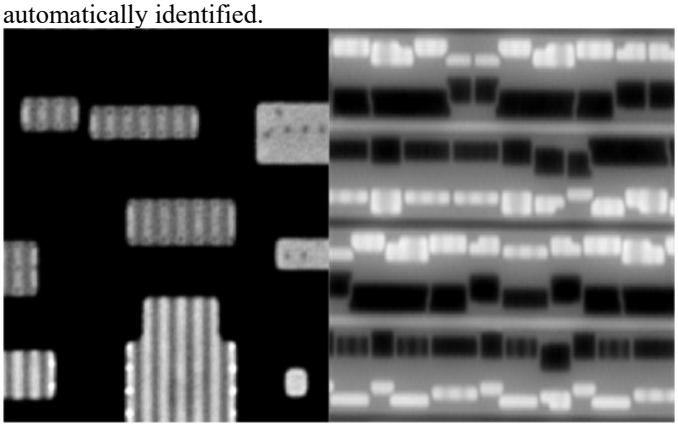
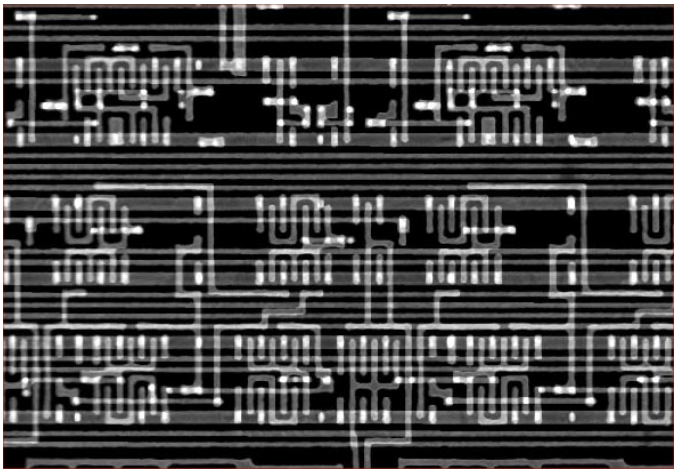


Figure 2: Left – Intrinsic Voltage Contrast, Right- Backside EBIC (Top) examples of implant imaging used to generate GDS II active layers.

Stitch / Overlay and Alignment of Layers

Software algorithms play a critical role to achieve near perfect SEM tile stitching, and interlayer alignment. Particularly for large MOSAIC's where SEM beam drift can play havoc during the collection of several hundred thousand tiles. The Raith chip scanner (CS), with a laser guided interferometer stage, is a good choice when it comes to the collection of larger MOSAICs.

Once the individual layers are captured, precision alignment is required to match up the interconnection of the stacked layers. This is accomplished using an anchored alignment system, which pins and reshapes the mosaic layers to achieve pixel level alignment.



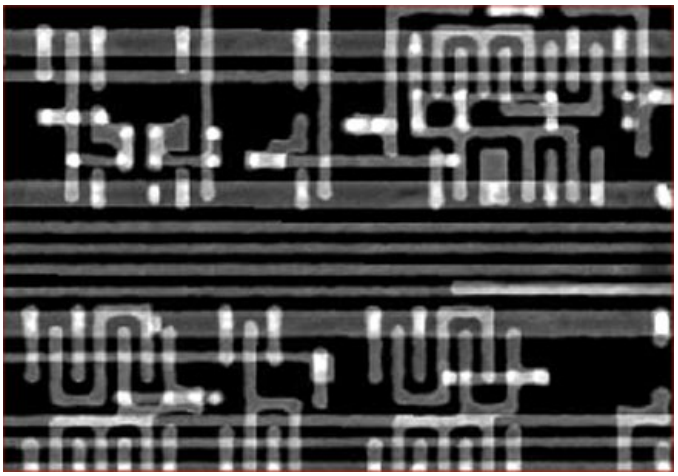


Figure 3: Overall and Close-up view showing interlayer alignment of metal and via layers.

GDS II Conversion

Going from the physical world to electrical models requires GDS II conversion. GDS II conversion is heavily dependent upon sample preparation, and cleanliness of the sample. Software can help a great deal when it comes to filtering unwanted artifacts, and highlighting the metal line or via features.

Figure 4: GDS II conversion of M1, via and M2.

.

Automated Library Cell Catalog Extraction:

Automated library cell extraction is done as follows –

1) Identify transistors using GDS II implant and polysilicon layers.
2) Identify Input and Output Library Ports
3) Netlist transistors and metal layers
4) Generate Truth Table / Database Comparison
5) Generate Verilog Models/ Schematics
6) Pattern Search and Place library Cell Instances

Automated Circuit Extraction Process Flow:

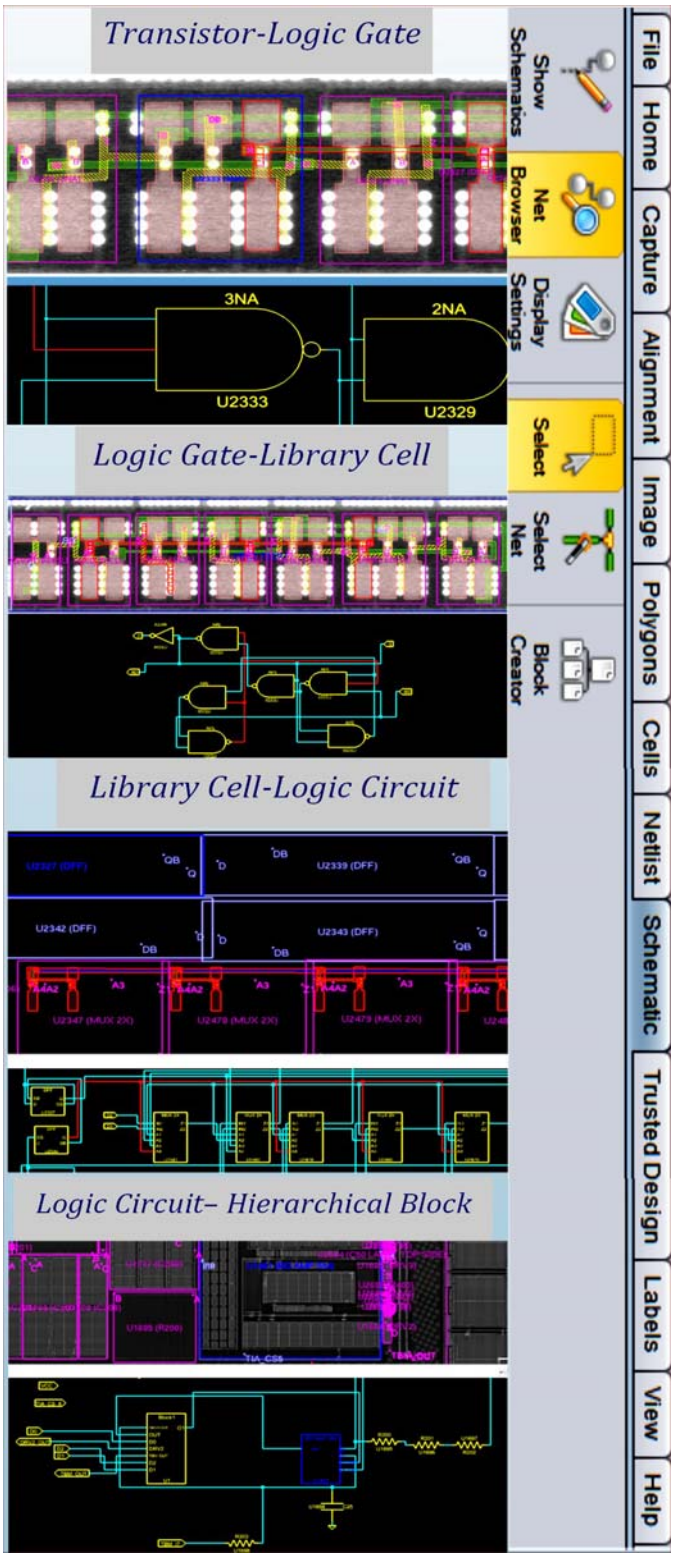


Figure 5: Process flow for automatic circuit and Hierarchical Block extraction.

Netlist – Schematic Generation:

Net Listing (Verilog, VHDL, or SPICE models) and Schematic are generated "real time" with the extraction of the GDS II layers and library cells. To extraction process is guided by polygon and electrical error checking. The Net List, library cell models/schematics can be imported to most common CAD tools for extended development work, such as transfer the design into a new technology which is commonly done on parts obsolescence projects.

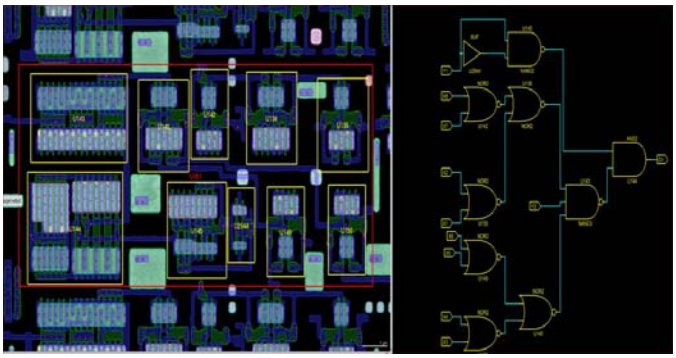


Figure 6: Library cells and schematic layout example.

Hierarchal Circuit Block Models:

IC design involves repeating circuit blocks that contain numerous library cells. Software algorithms allows us to store the net list of one of these Hierarchal instances, and similar to library cells, using netlist and pattern information, search and place Hierarchal Blocks. Hierarchal Blocks are key to helping us organize and simply the understanding of the functional models used to design the IC.

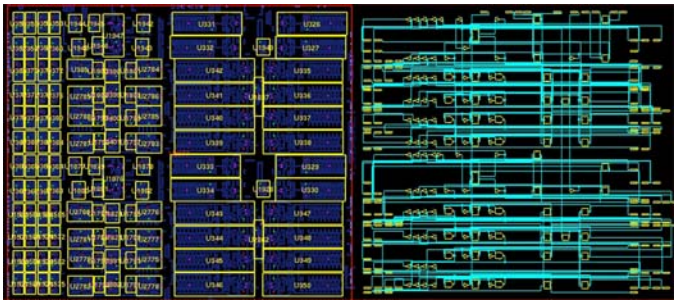


Figure 7: Hierarchal Circuit Block Organization.

Microcode Memory Extraction:

Reverse Engineering of complex circuits is much more than just duplicating the circuits on the die. It often requires extraction of the machine code and user specific code stored in ROM and/or Flash memory arrays. This microcode is usually well protected from invaders. Therefore extraction requires a thorough understanding of the memory array layout, encryption hardware and location of security bits.

Automated extraction of the "1"s and "0"s is accomplished using Software provided that the features can be distinguished as a "1" or "0".

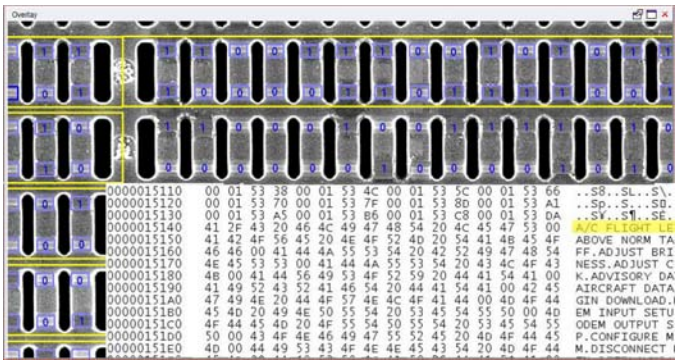


Figure 8: Automated Memory Code Extraction

Conclusions

To keep pace with reverse engineering state-of-the art microcircuits, an integrated software suite which automates going from the physical world (pictures) to an electrical model (Net List) is required. In this paper we discussed the process flow and the software automation that has been achieved to date.

Acknowledgments

Drew Jetter and Eric Henson, MicroNet Solutions software engineers.

References

[1] Randy Torrance, Dick James - The State of the Art in IC Reverse Engineering, International Association for Cryptologic 2007